ACME Company Cybersecurity Roadmap.

Acknowledgment

This material is based upon work supported by Roadrunner Corporation.

Disclaimer: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Table of Contents

Executive Summary

The cybersecurity landscape is complex, and the threats posed to ACME Company are real. Cyberattacks range in magnitude and impact and can occur in many forms, such as phishing attacks through employees' emails and gaining backdoor access to a utility's IT network through third-party vendors. These threats originate from a spectrum of malicious sources, ranging from individual actors to malicious actors. Establishing and managing a cybersecurity program can be difficult with complex IT and operating systems and limits on technical staff, however, it's a necessary precaution against cyberattacks of any kind.

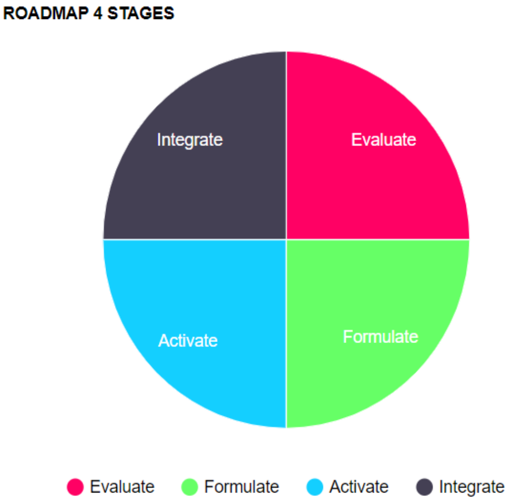
The ACME Company Cybersecurity Roadmap is a strategic plan designed to help ACME Company utilities develop a stronger, sustainable state of security that is continually monitored and improved upon. To ensure accuracy and applicability, the Roadrunner Corporation has developed the roadmap using input from public security, information technology, operational technology, and leadership experts.

The roadmap is built on the ACME Company Cybersecurity Scorecard, a tool to assess an organization's cybersecurity operations and practices. Using findings from the Scorecard, the Roadmap facilitates a path to an improved state of cybersecurity. It breaks down how to approach the broad and sometimes intimidating scope of cybersecurity practices into four distinct, manageable stages. As a utility moves through the Roadmap, the Scorecard can act as a useful standard by which to monitor and measure improvements to organizational cybersecurity practices.

The roadmap's four stages help utilities to set and achieve meaningful program goals.

STAGE 1:

EVALUATE internal and external factors influencing most pressing cybersecurity issues and identify two to three promising opportunities to target. ACME Company utility must conduct an initial risk-based assessment to define the current security posture and determine necessary means for achieving the desired future state. Such activities include identifying a target profile goal, gaining support from senior management, establishing a risk management plan, and establishing a project-based approach to cybersecurity.



STAGE 2:

FORMULATE a project-based plan to improve cybersecurity in two to three identified areas, being sure to define: a cybersecurity strategy, a clear schedule, data and metrics, a resource management plan, and the role of project lead. The overall project management plan should include: a project scope, a communications plan, a schedule, a budget, and a risk plan. ACME Company utility should review information technology (IT), operational technology (OT), and security organization workforce by defining the impacted roles and responsibilities of personnel within the utility. This stage also includes standing up processes to check key staff and vendor backgrounds to help a utility reduce its exposure to cybersecurity threats. Distinct management training, technical staff training, and non-technical staff training can prepare individuals within the organization.

STAGE 3:

ACTIVATE the project-based plan. This entails conducting the steps outlined in the plan, which might include installation of tools and systems used to monitor and secure IT and OT systems, as well as implementation of new security policies and procedures. ACME Company power utilities should adopt policies and practices that both the utility and individual personnel support to enable a culture of organizational security. Utilities can implement rewards to recognize good cybersecurity practices, as well as sanctions to provide corrective measures when practices are not executed. Utilities should also prepare for an incident response by putting in place the tools, practices, and communications to be deployed should an event occur. Implementing a series of risk management practices is key to performing advanced preparation for a cyber incident

STAGE 4:

INTEGRATE practices defined by the plan into the operation of the organization and make them a part of the organization's culture. If the project-based cybersecurity plan involved implementation of tools and systems to monitor and secure IT and OT, ensure these new tools are monitored regularly. Perform periodic tests and audits of these systems and conduct regular updates and maintenance. Share new processes and procedures with those responsible for maintaining them and those who must follow them. Consider performing security audits against new processes to ensure employees remain vigilant within the rewards and sanctions systems. Finally, revisit the ACME Company's Scorecard to reassess the organization's cybersecurity maturity and to prepare for further evaluation (and return to stage 1).

TEAM-WORK

The roadmap serves as a guide. This document provides insight into valuable and effective strategies for improved cybersecurity, but the success of any project lies in its execution. Tools and resources to engage peers and collaborate with the company subject matter experts are included in this document. The threat of a cyberattack may be very real, and the scope of cybersecurity may be daunting, but by working together we can improve the cybersecurity of the entire public power sector and continue to provide the best services to our communities and customers for years to come.

Introduction:

ACME Company utilities face many evolving challenges. Prominent among these is the threat of cyberattack and the corresponding duties of developing and executing an effective cybersecurity program. Rapidly evolving technologies at all operational levels' present potential targets for attack and substantial liabilities if compromised. Although organizational leadership is ultimately responsible for executing the strategy and securing the resources to appropriately address cybersecurity threats, all personnel must understand and appreciate their role in ensuring the security of their organization. This document provides materials and strategies by which to design, launch, and monitor a multi-year program to improve organizational cybersecurity.

The Cybersecurity Threat to ACME Company.

Cybersecurity is a growing global concern. Interconnected technological systems enter our daily lives, increasing efficiency and modernizing our business operations. These systems also increase vulnerabilities through third parties, data breaches, supply chain practices, natural disasters, and unintentional employee disclosures.

Small and medium public power organizations face many of the same threats and vulnerabilities as larger utilities and yet must address these using limited resources. ACME Company's utilities are responsible for critical infrastructure and are widely interconnected with many loosely affiliated (or completely unaffiliated) organizations.

About this Roadmap

The ACME Company Cybersecurity Roadmap builds on the Scorecard by assisting organizations to develop a strategic plan that prioritizes and details appropriate elements of a cybersecurity program. Together, the Scorecard and the Roadmap provide a strategic framework to help utilities plan and deploy cybersecurity efforts over the next three to five years. This framework draws on peer organization experience and cybersecurity expert knowledge to distill the volume of cybersecurity information in to clear, tangible strategies to gain support, ensure buy-in, and create an organizational culture that embraces secure practices as part of everyday habits.

To successfully achieve the program goals, the Roadrunner Corporation team identified four stages through which organizations can build and deploy their efforts. Cumulatively, these efforts provide the framework for organizations to provide their communities with responsible, secure cyber practices and respond to incidents efficiently and effectively.

Stage 1- Evaluate

EVALUATE internal and external factors influencing most pressing cybersecurity issues (i.e. complete the Scorecard assessment), locate sponsors and leaders needed to achieve desired changes, generate a list of prioritized opportunities for improving cybersecurity and consider the organization's strategy and risk tolerance.

Inputs:

- ACME Company's Vulnerability Scan scorecard.
- Existing cybersecurity processes and procedures
- Personnel training and awareness.

Processes:

- Gain initial support for cybersecurity efforts from sponsors and stake holders.
- Use Scorecard to evaluate organizational processes.
- Generate list of goals for improving cybersecurity and use a risk-based approach to identify two or three opportunities for improving cybersecurity from these goals.
- Define the means to achieve these goals and gain funding.

Outputs:

- Two or three defined, achievable goals that will improve the organization's Cybersecurity.
- Endorsement of project by relevant sponsors.

Sponsorship, Stakeholders And Givens

Gaining support from leadership is an important first step in any major initiative and is especially critical for a cybersecurity program at ACME Company, since ACME has seen more industry partners and suppliers compromised in the last two years, and this has raised the C-Suite's awareness to build a more Risk-based approach, but they have not implemented the Risk framework. The company has invested in a future hire for a Chief Risk Officer comprising Information Security, Physical Security, and Supply chain security.

The Roadrunner Corporation team underscored the importance of this step many times, indicating that without leadership support, any cybersecurity improvement effort is unlikely to succeed.

Identify a sponsor

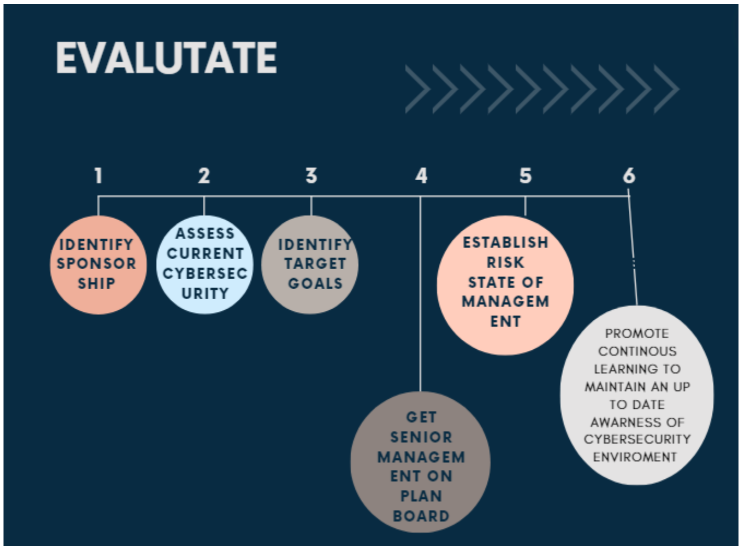
As with many programs that introduce the potential for significant change, cybersecurity programs benefit greatly from a defined sponsor. This individual's primary role is to help garner support, overcome barriers, and serve as an interface for senior stakeholders who have an interest in the program. Additionally, sponsors can identify resources and provide clear delegation of cybersecurity duties among staff. Ideally, given their role, the sponsor is positioned to assign resources across the organization. For example, while many utilities may organizationally separate Information Technology (IT) and Operations Technology (OT) departments, the Roadrunner team identified the importance of identifying a cybersecurity project sponsor with clear authority over resources in both IT and OT organizations.

While the sponsor does not initially need to have a deep understanding of cybersecurity solutions, this individual can serve as a sounding board for the cybersecurity project leader. The sponsor can assist by using his or her experience with the utility and its strategic objectives and understanding of potential operational and customer impacts of any cybersecurity improvements suggested by the team.

MAP OUT STAKEHOLDERS

Like a significant project, cybersecurity improvement projects have many stakeholders—individuals or groups who have an interest in or can influence the outcome of a project. Sponsors and identified project leads should spend time identifying any cybersecurity project stakeholders and consider their potential questions, positions, and reasons for support or resistance to the project. Understanding the objectives and concerns of the various stakeholders in the cybersecurity program development is important for it to succeed.

Examples of stakeholders include elected officials such as the city council, regulators, consumer advocacy groups or key customers in the service territory, vendors who provide cybersecurity services or technology, and staff who need to abide by new policies or processes. Building even a short list of these stakeholders and considering their positions and objectives on cybersecurity investment and process changes will aid the team immensely as proposals for projects and initiatives are considered and reviewed with utility decision makers.


EVALUTATE
1
2
3
4
5
6
IDENTIFY SPONSOR SHIP
ASSESS CURRENT CYBERSEC URITY
IDENTIFY TARGET GOALS
GET SENIOR MANAGEM ENT ON PLAN BOARD
ESTABLISH RISK STATE OF MANAGEM ENT
PROMOTE CONTINOUS LEARNING TO MAINTAIN AN UP TO DATE AWARNESS OF CYBERSECURITY ENVIROMENT

RESEARCH GIVENS: REGULATIONS, LAWS, AND STANDARDS

Getting to know the "lay of the land" for cybersecurity will help to set the tone of and understanding for the activities to come. The sponsor or project lead should have an initial understanding of the regulations, laws, and standards that could impact a cybersecurity program. Resources from previous projects that address cyber or physical security are a good place to start.

Public power entities can explore other initiatives within their municipality or government (e.g., police department initiatives related to improving secure communications or patient data privacy compliance required for first responders). the sponsor or project lead can look to peer utilities that have recently begun cybersecurity initiatives or to the Board meetings. This stage will help a utility understand the state of its cybersecurity, identify what steps it needs to take to develop a clear plan to improve cybersecurity, gain the support it needs to put the plan into action, and manage an ongoing cybersecurity project.

Initial Assessment Activities

Assess cybersecurity posture

It is essential to develop a clear and complete understanding of an organization's cybersecurity environment. This entails both the internal and external environments. The internal environment addresses the organization's operations, including relevant personnel, their responsibilities, and the hardware, software, and infrastructure they engage with while working. The external environment includes relevant regulations, interconnections with other organizations, and any other outside factors that might influence operations. The ACME Company's Cybersecurity Scorecard provides a clear measure of organizational operations and identifies gaps that are good targets for initial improvement efforts.

Baseline Assessment Activities

- Identify and engage other business units.
- Define Scope of assessment
  1. Physical building
  2. Systems
  3. Applications
  4. External services
  5. Staff members.
- Inform all involved of the purpose of the effort and what is expected of them.
- Schedule document and interview requests
- Engage existing tool: Vulnerabilities Scan Assessment
- Enlist a professional, independent, and onsite assessment
- Perform independent penetration test
- Perform any additional current state assessments of IT, OT, User Management, Profiles and Passwords.

Identify Target Profile Activities

- Cybersecurity center of Excellence Program
- Benchmark against similar Utilities.
- Estimate cost and benefits for targets
- Review existing standards, identify milestones (1/2 year to annual frequency).

Develop a Target profile (Goal)

Once the initial assessment is completed, the project can be mapped. This involves developing a strategic plan for improving an organization's cybersecurity over the next three to five years. The plan must include clear, actionable steps and strategies and means of accountability to ensure it is used.

Outline a business case and seek buy in

A plan has no value unless it is put into action.Buy-in from senior management, the board, and other members of the guiding coalition helps to address two of the largest concerns for project success: 1) organization personnel and other internal stakeholders will resist the plan, and 2) organization leadership will not sufficiently support or enforce the plan. Engaging organizational leadership requires careful definition of the goals and scope of the plan and a clear business case for the project.

Making the case

- Define what we are trying to protect.
- Develop business case
    - i. Outcomes of penetration test.
    - ii. Examples of incidents
    - iii. Include benchmark assessment.
- Use Scorecard to identify target for cyber program (end-goal for phase)
- Identify budget and resource needs
- Identify peer/mature utilities for guidance
- Enlist outside consultants
- Identify and recruit ‘cyber council’ (management, tech management, physical security, technicians)

Risk Management Checklist

- Integrate with Enterprise Risk Management
- Consult or develop risk register
- Rank cyber risks relative to enterprise risks
- Identify a champion in the existing Enterprise Risk Management Process

  Perform risk assessment
- Define threats
- Identify assets
- Review vulnerabilities
- Analyze risks
- Prioritize risks analyzed (*high/medium/low*)
- Create risk remediation recommendations

Risk Analysis Checklist

- Assess “brand risk” exposure
- Assess compliance/regulatory risks
- Create realistic risk measures
- Examine corporate risk tolerance
- Review policies (e.g. access policies) to determine non-negotiable risk exposure
- Consider quick wins
- Define risk in business/management terms

Cybersecurity is a rapidly evolving field, a new development in technology and changing risks. Staying aware of the cybersecurity environment demands a dedicated, but not overwhelming, effort. Conferences, exercises, and training are essential to continuous learning. Online training programs can be scheduled and budget-friendly ways to learn about best practices and newest developments from industry experts. Include all levels of staff in these training courses to underscore the importance of cybersecurity in the organization’s culture. The Association can guide utilities to proven and current training resources. Though more expensive and demanding of time, attending conferences and in-person trainings provides unparalleled value in interaction with peers from other organizations and cybersecurity experts, which can improve one’s understanding and ability to apply the latest tools and techniques. The project lead should attend at least one such event per year, and other project leads and/or task leaders should be encouraged and enabled to attend as well. The company that can develop in such an experience is invaluable to a constructive and enthusiastic organizational culture.

Stage 2-Formulate

FORMULATE a project-based plan to improve cybersecurity; use a risk-based approach to identify two or three promising opportunities for improving cybersecurity; appoint leadership and hire appropriate staff to carry out cybersecurity efforts and implement managerial, technical, and general staff training.

Inputs:

- Defined goals for improving cybersecurity
- Support from sponsors and leadership

Processes:

- Generate a project-based plan by which to achieve the priority goals
- Build plan starting with the current state of cybersecurity
- Identify relevant milestones by which to mark and measure progress

Outputs:

- An actionable plan project leaders and process-level personnel can use to understand the goals, purposes, and needs for each stage of the project

Establish a Project-based Approach

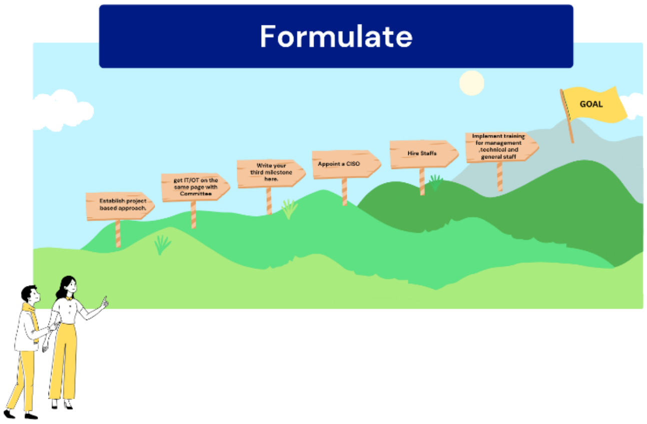
Applying project management techniques and concepts to a cybersecurity improvement effort can provide utilities with a familiar framework and proven methodology for implementing a new program. Using the familiar touchstones of project management communicating goals, setting a schedule to achieve those goals, developing tools to facilitate the plan, and continuing to learn about the pursuit can clarify cybersecurity and better ensure success.

Develop a cybersecurity strategy

A strategy requires a goal, and setting cybersecurity centric goals builds cybersecurity into both the organization's aspirations and culture.

Create a clear schedule

Create a clear schedule to guide the maturation of the project and provide clear milestones by which to mark progress. Strategies with the greatest likelihood of success seem to be built on a timeframe of three to five years, long enough for a program to mature and develop, but immediate enough to afford urgency and limit scope to a tangible set of activities. Prioritize actions and then develop a schedule to reach desired milestones within the set timeframe.


Formulate
GOAL
Establish project based approach.
get IT/OT on the same page with Committee
Write your third milestone here.
Appoint a CISO
Hire Staffs
Implement training for management ,technical and general staff

allocation of resources to a project. A resource management plan influences the management of how financial, personnel, and vendor resources get applied to a project. Allocation of human resources requires a clearly defined set of responsibilities and roles for each staff member and for vendors and outside consultants. As cybersecurity is a feature of organizational culture, all personnel should play some role, and all vendors and suppliers identify should likewise have a clear role to play for which they will be held accountable.

Project-Based Approach

- Define cybersecurity strategy as a corporate goal
- Develop prioritized action list with dates, responsible parties, and resource estimations
- Define data and metrics for security program
- Develop resource management plan (budget, personnel and vendors)
- Create cyber project management plan
    - Communications plan
    - Scope
    - Schedule • Budget
    - Risk plan
- Engage in continuous learning
    - Ongoing training programs (all levels of personnel)
    - Exercises/conferences/training

Workforce Development Checklist

- Review IT, OT, and Security Organization

  Found an IT/OT Bridge Committee

  Designate a Cybersecurity information Security Officer

  Put federal resources into use
- Hiring Practices
- Supply Chain Risk (Vendor) Management

  Background checks

  Vendor tracking

  Security Controls in Contracts

  Security Controls for Communications

Workforce Development checklist

(Management -level.)

- Cybersecurity literacy
- Operational capabilities and limitations
- Communication strategies during an incident
- Held in conjunction with local government stakeholders

Workforce Development Checklist:

(Technical Staff Training)

- Lunch and learn sessions to align efforts of IT and security staff
- General Staff Training
- Online training to introduce (and refresh) cybersecurity basics
- Quarterly workshops to address specialized topics
- Compliance and good “hygiene” are rewarded

Stage 3- Activate

ACTIVATE the project-based plan by creating ongoing, enforceable policies for all personnel; follow the activities or steps identified in the plan, acquire any necessary new tools or systems then install and test them, institute new policies and procedures needed to support tools and identify improvements to cybersecurity processes and design a communications strategy to handle potential cyber incidents.

Inputs:

- Project-based plan to improve cybersecurity

Processes:

- Use the plan as a guide to launch new practices, policies, and protocols; conduct activities noted in the plan.
- Review and revise policies to enforce new practices, including rewarding compliance and penalizing noncompliance

Outputs:

- New organizational standards for practice and behavior that help the organization achieve its cybersecurity goals
- New tools and systems to enforce standards and reduce risk

Policies

A comprehensive, policy-driven approach is necessary to enforce the desired shift in organizational culture. Even with trained and vetted personnel, the organization must afford its commitment to security with on-going, enforceable policies that all personnel adopt and follow. Policies must ensure that practices by both the utility and individual personnel.

Thoroughly test any new tools or systems to be installed and used, both for functionality and for system impact. Each new system will include a new set of policies and procedures that must be developed for adoption by the organization. This includes procedures for system use (e.g., monitoring system logs) and plans for system maintenance to ensure it continues to offer appropriate monitoring and security.

However, an organized approach to policy development should start with the recognition or adoption of a cybersecurity framework. Document all knowledge generated from these new policies for use by relevant personnel. Maintaining knowledge and accountability of practices can improve communication and awareness among relevant employees and aid future forensic investigations.

Workforce Development Checklist

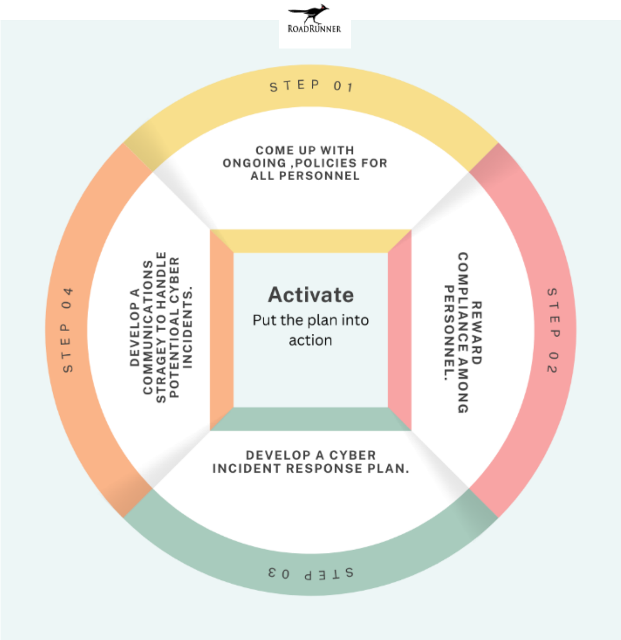
(Policies, Rewards, and Sanctions)

- Policies
- Security Assessments
- Scanning kiosks
- Cybersecurity newsletter
- Strengthen personnel password policies
- Document all new policies for easy reference
- Rewards and Sanctions
- Recognition of good "hygiene" practices presented with an audience.
- Corrective measures communicated in confidence.

Rewards and sanctions

As mentioned in the "Training" section, certificates or similar recognition of good hygiene and practices offer useful means of rewarding compliance and communicating that leadership are monitoring compliance (and lack thereof). This underscores the need for everyone in the organization to honor and respond to policies and practices. Other methods of rewarding compliance or sanctioning non-compliant personnel can be tailored to the culture of an organization. Employees can be rewarded with premier parking spaces, gift certificates and cybersecurity employee of the month recognition.

Sanctions must also be devised and clearly communicated to all employees to enforce that compliance is not optional or limited to a select subset of personnel. Sanctions should begin with private, one-on-one conversations when inappropriate activities are recognized, and escalate as needed. The purpose of sanctions is to correct behavior, not to publicly shame personnel.


ROADRUNNER
STEP 01
COME UP WITH ONGOING ,POLICIES FOR ALL PERSONNEL
STEP 02
REWARD COMPLIANCE AMONG PERSONNEL.
Activate
Put the plan into action
STEP 03
DEVELOP A CYBER INCIDENT RESPONSE PLAN.
STEP 04
DEVELOP A COMMUNICATIONS STRAGEY TO HANDLE POTENTIAL CYBER INCIDENTS.

Incident Response

The true test of a cybersecurity program is incident response to an actual breach. A utility is either prepared for an incident or it is not. Developing and executing a cyber incident response plan is a key component for any organization, especially an electric utility. Implementing a series of risk management best practices will lay the foundation for preventing cyber related attacks. Assembling the right people with a clear chain of command, procuring the right tools and support, and networking with key outside stakeholders is crucial for success. This suite of actions helps secure a utility's network and build trust within and outside its organization, as well as prepares the utility's team to handle any cyber threat that may come its way. The team should include an overall team manager and technical staff, plus individuals who can maintain and update all lists, strategies, and the overall cybersecurity plan.

Detect and Respond to Cybersecurity Incidents

The Playbook details the steps required to detect and identify potential cyber incidents. Containing an incident is a utility's immediate priority, the Playbook includes metrics to help a utility categorize and prioritize (ranging from Levels 0 to 5) the incident to determine the type of impact it made on the utility.

The Playbook outlines the steps necessary to escalate and report an incident, including engaging internal stakeholders, gathering evidence, and conducting initial containment. Investigating, developing resource solutions, and eliminating an incident are also key actions when responding to an incident. In addition to the actions described in the Playbook, a utility might also consider using a form to track an incident from start to finish to assist with lessons learned during debriefing and, when recovering from an incident, developing specific actions for fixing, patching, and/or stopping the security breach.

Communicating During a Cyber Incident

A strong communications structure to be used during a cyber incident can mean the difference between effective and ineffective responses. The flow and content of communications during a cyber incident will likely be different for internal and external stakeholders. Communications functions are essential both in normal operation and crisis response and must be carefully planned for quick and effective deployment. Building cyber awareness and related topics into regular communications can project subject authority to internal and external audiences and introduce the subject as an important and carefully considered to organizational operations. Internal communications focus on how to address the board, management, and personnel.

An internal communications plan is necessary to keep employees and other key stakeholders in touch with the happenings of a cyber incident.

External communications address customers, communities, interconnected peer organizations, and regulatory and oversight agencies, among others. Regular business as usual communication with customers and communities can cultivate a healthy relationship better able to weather a crisis event.

Stage 4 – Integrate

INTEGRATE practices defined by the plan into the operation of your organization, move new tools or systems into the production environment, ensure any new systems are regularly monitored and regular patches and upgrades are maintained, operationalize and maintain the new process as part of business-as-usual practices. This turns the “new” practices into “standard” practices making them part of your organization’s culture is the final critical stage in improving cybersecurity and making sure the improvements last.

Inputs:

- New policies, procedures, tools, or systems that enforce the desired improvements to cybersecurity from the project-based plan

Processes:

- Move new tools and systems into production environment and continue to operate and maintain them
- Operationalize and maintain the new processes as part of business-as-usual practices; this turns the “new” practices into “standard” practices
- Make the new behaviors part of the organization’s culture to ensure changes last

Outputs:

- Achievement of the goals of the project-based plan
- New culture of cybersecurity ready for assessment via Scorecard and other tools to identify additional improvements to target.

Systems

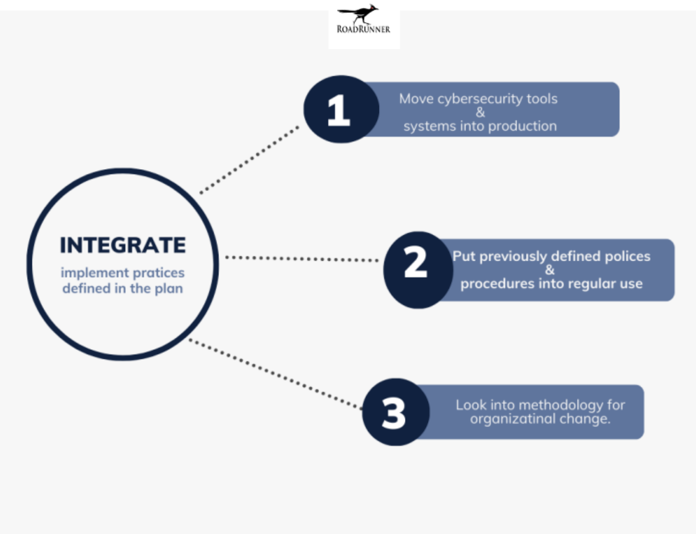
Cybersecurity protection, monitoring, or maintenance systems that have been tested and installed into the organization’s IT and OT environment should be moved into production at this stage. Pay special attention to the impact that monitoring tools have on existing operational systems in a production environment. Some solutions include so-called “passive” monitoring to limit interference with standard operations. During integration and activation of any tool, it is critical that the project team assure there are no undue impacts on operations. At this stage, the project team hands operation of new tools over to operations staff or maintains systems that are its responsibility

Policies and Procedures

At this point, the policies and procedures identified and laid out earlier are moved into regular use. Given the operational nature of ACME Company, many organizations maintain written policies and procedures for IT, OT, and business and personnel functions. These procedural sources are also appropriate locations for cybersecurity policies and procedures. However, given the innovation of these procedures, related stakeholders that haven’t been exposed to the new practices will need training, and organizations will need to implement practices for sharing these procedures with new staff and vendors.

Organizational Adoption and Culture Change

As mentioned earlier in this Roadmap, perhaps the most challenging aspect of cybersecurity is behavior change. The Roadrunner team recommended that ACME Company look into and apply a methodology for organizational change management based on what works for their organization. In the context of a cybersecurity improvement plan, this Roadmap acknowledges these recommended change management steps from the beginning by engaging management and enrolling assistance from across the organization. Training and development steps identified in earlier stages build knowledge and skills among staff. Ultimately, and most important to any cybersecurity improvement program, reinforcement of the changes can occur through continued staff awareness and training, as well as by revisiting the ACME company’s Vulnerability Scan assessment to determine the organization’s next risk-based targets.


ROADRUNNER
INTEGRATE
implement pratices defined in the plan
1
Move cybersecurity tools & systems into production
2
Put previously defined polices & procedures into regular use
3
Look into methodology for organizatinal change.

Roadmap Next steps

The guidance provided via this Roadmap is intended to promote improvement and ongoing maintenance and vigilance of critical infrastructure and private customer data. The roadmap's stages and recommendations reflect input from individuals representing ACME Company that have prepared for, been exposed to, or addressed security threats in the hopes that others may learn and act. The Roadrunner team members recommend maintaining a posture of continuous cybersecurity improvement, no matter the size of the ACME Company. The Company can follow this recommendation by taking advantage of the resources and tools referenced in this document, including the Vulnerability Scan assessment. For the latest recommendations, visit the Association's website at www.roadrunnercorp.org or email Cybersecurity@roadrunnercorp.org.

Reading this document can provide insight into valuable and effective strategies for improved cybersecurity, but the success of any project lies in its execution. Communication among peers and collaboration with the Association and experienced subject matter experts might be necessary, and the tools to engage those resources are included in this document. The threat of a cyberattack may be very real and the scope of cybersecurity may be daunting, but by working together, we can improve the cybersecurity of the company and continue to provide the best services to our communities and customers for years to come.

Appendix A: Example CISO Job Description

A Chief Information Security Officer (CISO) is the executive-level manager who directs the organization's cybersecurity strategy and budget and governs the cybersecurity information and system operations protection. The scope of responsibility holds policy, communications, training, procurement, development, infrastructure, systems, and applications.

Related Position Title

Other titles used to describe this position include:

- Chief Security Officer (typically also includes physical security responsibilities)
- Corporate Security Executive
- Information Security Director (may not be an executive-level position)
- Corporate Security Officer (may not be an executive-level position)
- Information Security Officer (typically not an executive-level position)
- Information Security Manager (not an executive level-position; may not have budget)
- Information Systems Security Manager (responsibility typically limited to systems)

In small- to medium-sized organizations, the CISO responsibilities may be part of an existing executive level position such as CEO or CIO.

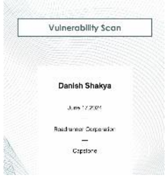
CISO Responsibilities & Duties

The CISO and the CISO team typically are responsible for the following:

- Strategy: Create, manage, and update the organization's cyber security strategy to address organizational cybersecurity concerns, threats, regulations, and technology.
- Policy: Direct, create and manage information security policies and standards; direct and approve information security procedures.
- Requirements: Define and advice regarding the implementation of cybersecurity requirements for existing and developed applications and outsourced services.
- Design: Consult and advise how to incorporate adequate security controls into system designs.
- Assess: Ensure adequate cybersecurity assessments of existing controls, including security risk assessments, vulnerability scanning, penetration testing, code review, user rights reviews, and compliance gap assessments.
- Mitigate Risk: Design, advise, and oversee the revision or creation of cybersecurity controls adequate to address known cybersecurity risks consistent with the risk appetite of the organization.
- Log and Monitor: Ensure appropriate application and system logging takes place and that these logs are reviewed for cybersecurity incidents.
- Investigate: Direct cybersecurity incidents, disclosures, or breach investigations, including impact analysis and appropriate internal notifications.
- Response: Ensure effective response and lessons learned to cybersecurity incidents, disclosures, and breaches.
- Communicate: Appropriately communicate externally in response to disclosures and breaches.
- Continuity: Ensure disaster recovery and business continuity plans incorporate adequate cybersecurity controls and are tested and updated.
- Compliance: Ensure cybersecurity compliance with relevant laws, regulations, standards and contracts
- Vendor Management: Manage cybersecurity requirements and oversight of vendors providing services to the organization.
- Threat Intelligence: Maintain a current understanding of relevant cybersecurity threats impacting the industry and the organization.
- Security Awareness: Ensure all personnel receive effective security awareness training and updates.
- Inform Board: Communicate cybersecurity risks and strategy to board members and executive committee and address concerns.

Appendix B: Vulnerability Scan Assessment

- Vulnerability Scan Assessment



Vulnerability Scan

Danish Shakya

June 17 2024

Roadrunner Corporation

—

Capstone

Link to the assessment